Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.408 – 417

RESEARCH ARTICLE

An Overview of MANET: Applications, Attacks and Challenges

[1]Mr. L Raja, [2]Capt. Dr. S Santhosh Baboo

[1]Assistant Professor, Dept. of Computer Applications, Pachaiyappa's College, Chenni-30,
[2]Associate Professor, P.G. Research Dept. of Computer Science, D.G. Vaishnav College, Chennai-106
[1] lakshraja1@yahoo.com, [2] santhos2001@sify.com

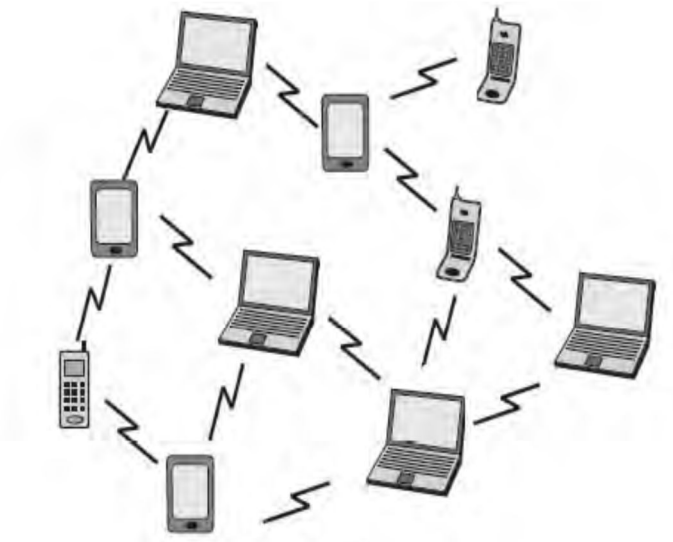
Abstract:

Advancement in the field of internet due to wireless networking technologies gives rise to many new applications. Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications. This paper provides insight into the potential applications of ad hoc networks, various attacks and discusses the technological challenges that protocol designers and network developers are faced with.

Keyword : MANET; Applications; Attacks and Challenges

1. Introduction:

MANET is a self configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move haphazardly and organize themselves arbitrarily. Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET. MANET have given rise to many applications like Tactical networks, Wireless Sensor Network, Data Networks, Device Networks, etc. With many applications there are still some design issues and challenges to overcome. The main goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes which may be combined routers and hosts--they form the network routing infrastructure in an ad hoc fashion. Lot of security vulnerabilities in a wireless environment, such as MANET, has been identified and a set of countermeasures were also proposed. However, only a few of them provide a guaranty which is an orthogonal to security critical challenge. Taking these factors into concern, the main vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links.



Mobile ad hoc network

MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of

centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks.

2. History of MANET:

Basically, MANET can be categorized into first, second and third generations. The first generation came up with "packet radio" networks (PRNET), and were sponsored by DARPA in the early 1970s. It has evolved to be a robust, reliable , operational experimental network. The PRNET used a combination of ALOHA and CSMA approaches for medium access, and a kind of distance-vector routing to provide packet-switched networking to mobile battlefield elements in an infrastructureless, hostile environment. The second generation evolved in early 1980's when SURAN (Survivable Adaptive Radio Networks) significantly improved upon the radios (making them smaller, cheaper, power-thrifty), scalability of algorithms, and resilience to electronic attacks. Important developments during this period include GloMo (Global Mobile Information System) and NTDR (Near Term Digital Radio) The goal of GloMo was to provide office-environment Ethernet-type multimedia connectivity anytime, anywhere, in handheld devices. Channel access approaches were now in the CSMA/CA and TDMA molds, and several novel routing and topology control schemes were developed. The NTDR used clustering and link- state routing, and self-organized into a two-tier ad hoc network. Now used by the US Army, NTDR is the only "real" (non-prototypical) ad hoc network in use today. The third generation evolved in 1990's also termed as commercial network with the advent of Notebooks computers, open source software and equipments based on RF and infrared. IEEE 802.11 subcommittee adopted the term "ad hoc networks." And the concept of commercial (non-military) ad hoc networking had arrived. Within the IETF, the Mobile Ad Hoc Networking (MANET) working group was horn, and sought to standardize routing protocols for ad hoc networks. The development of routing within the MANET working group and the larger community forked into reactive (routes on- demand) and proactive (routes ready-to-use) routing protocols 141. The 802.1 1 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable, if not optimal, for building mobile ad hoc network prototypes out of notebooks and 802.11 PCMCIA cards. HIPERLAN and Bluetooth were some other standards that addressed and benefited ad hoc networking.

3. Applications of MANET:

With the increase of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications in the commercial, Military and private sectors. Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure. This offers an advantageous decentralized character to the network. Decentralization makes the networks more flexible and more robust.

Military Sector : Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field

Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. This may be because all of the equipment was destroyed, or perhaps because the region is too remote. Rescuers must be able to communicate in order to make the best use of their energy, but also to maintain safety. By automatically establishing a data network with the communications equipment that the rescuers are already carrying, their job made easier. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

Low Level: Appropriate low level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

Data Networks: A commercial application for MANETs includes ubiquitous computing. By allowing computers to forward data for others, data networks may be extended far beyond the usual reach of installed infrastructure. Networks may be made more widely available and easier to use.

Sensor Networks: This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad-hoc sensor networks could be the key to future homeland security.

4. Attacks in MANET:

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified as in the following table

MANET security Layer	Attacks
Application Layer	Malicious code, Repudiation
Transport Layer	Session hijacking, SYN Flooding

Network Layer	Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing etc.
Data Link Layer	Traffic analysis and monitoring.
Physical Layer	Traffic Jamming, Eavesdropping

Attacks on mobile ad hoc networks can be classified into following two categories: Passive and Active attacks.

***1*) Passive attack:** in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information . This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered.

Snooping: Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism. Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function.

2) **Active attack:** in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker’s threat can be performed

Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance . For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

Black hole Attack: Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough route, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole .In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

Gray-hole attack: This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

Link spoofing attack: In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

Malicious code attacks: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

Repudiation attacks: Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

Session Hijacking: Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc.) and other information from nodes. Session hijacking attacks are also known as address attack which make effect on OLSR protocol. The TCP-ACK storm problem may occur when malicious node launches a TCP session hijacking attack.

SYN Flooding Attack: The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection are never completes the handshake to fully open the connection.

Denial of service attack: Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network

Jamming: Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

Selfish Misbehavior of Nodes: Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network. It may include two important factors. Conservation of battery power Gaining unfair share of bandwidth.

Traffic monitoring and analysis: Traffic monitoring and analysis can be deployed to identify the communication parties and functionalities, which could provide information to launch further attacks. Since these attacks are not specific to the MANET, other wireless networks, such as the cellular network, satellite network, and WLAN also suffer from these potential vulnerabilities. We did not focus on attacks on this layer for the security of MANET.

5. Challenges in MANET:

A. **Autonomous-** No centralized administration entity is available to manage the operation of the different mobile nodes.

B. Dynamic topology- Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

C. Device discovery- Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

D. Bandwidth optimization- Wireless links have significantly lower capacity than the wired links. Routing protocols in wireless networks always use the bandwidth in an optimal manner by keeping the overhead as low as possible. The limited transmission range also imposes a

constraint on routing protocols in maintaining the topological information. Especially in MANETS due to frequent changes in topology, maintaining the topological information at all nodes involves more control overhead which, in turn, results in more bandwidth wastage.

E. Limited resources - Mobile nodes rely on battery power, which is a scarce resource. Also storage capacity and power are severely limited.

F. Scalability- Scalability can be broadly defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.

G. Limited physical security- Mobility implies higher security risks such as peer-to- peer network architecture or a shared wireless medium accessible to both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.

H. Infrastructure-less and self operated- Self healing feature demands MANET should realign itself to blanket any node moving out of its range.

I. Poor Transmission Quality- This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

J. Ad hoc addressing- Challenges in standard addressing scheme to be implemented.

K. Network configuration- The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links.

L. Topology maintenance- Updating information of dynamic links among nodes in MANETs is a major challenge.

Conclusion

The evolution in the field of mobile computing is driving a new alternative way for mobile communication, in which mobile devices form a self-creating, self-organising and self-administering wireless network, called a *mobile ad hoc network.* Mobile Ad hoc networks are generally more vulnerable to physical security threats than fixed or hardwired networks. This paper throws a light on different concepts of MANETS that can help researchers to the maximum. Its intrinsic flexibility, lack of infrastructure, ease of deployment, auto-configuration, low cost and potential applications make it an essential part of future pervasive computing environments. As the involvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all forms. In all, although the widespread deployment of ad- hoc networks is still year away, the research in this field will continue being very active and imaginative.

References

[1] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester " An Overview of Mobile ad hoc Netwroks: Applications & Challenges ."

[2] K. Sanzgiri, B. Dahill, B.N. Levine, C. shield and E.M Belding- Royar, A secure routing protocol for Ad Hoc Networks, in Proceedings of ICNP'02,2002.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Wireless Communications, IEEE In Wireless Communications, IEEE, Vol. 14, No. 5. (06 December 2007), pp. 85-91.

[4] Krishna Moorthy Sivalingam, "Tutorial on Mobile Ad Hoc Networks", 2003.

[5] B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks," IEEE GLOBECOM '06.

[6] Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Workshop on Real-World Wireless Sensor Networks, June 20–21, 2005.

[7] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, Vol. 24, No. 2, Feb. 2006.

[8] HaoYang, Haiyun & Fan Ye — Security in mobile ad-hoc networks : Challenges and solutions,||, Pg. 38-47, Vol 11, issue 1, Feb 2004.

[9] Buttyan, L., and Hubaux, J. P. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*: Special Issue on Mobile Ad Hoc Networks, **8**(5), 2003.

[10] S. Corson and J. Macker, "RFC 2501 - Mobile Ad Hoc Networking (MANET): Routing Protocol Pe", Network Working Group, Request for Comments: 2501, University of Maryland, Naval Research Laboratory, JAN 1999.

[11] Ad hoc Networking, C.E. Perkins, Addison Wesley, Jan. 2001.

[12] C-K Toh, "Future Application Scenarios for MANET-Based Intelligent Transportation Systems", Proc. of Future Gen. Comms and Networking (FGCN 2007) - Vol. 2, p. 414-417.

[13] Shiv Rama Murthi and Prasad " Adhoc Wireless network" page no. 249-252, First edition, PHI, 2004

[14] R. Ramanathan and J. Redi, "A Brief Overview of ad hoc networks: challenges and Directions," IEEE Commun. Mag., vol. 40, no. 5, May. 2002.

[15] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, **1**(1), 2003, pp. 13–64.

[16] M. Grossglauser and D. Tse, "Mobility increases the capacity of ad hoc wireless networks", IEEE/ACM Transactions on Networking, Vol. 10, No. 4, August 2002.

